DIGITALT SITUASJONSBILDE

Kommune-CSIRT

Rapport nr. 3 – 2021

Rapporten er Kommune-CSIRT(K-CSIRT) sin beskrivelse og vurdering/analyse av digitale trusler, sårbarheter og hendelser i kommunal og fylkeskommunal sektor. Perioden for analysen er fra september til desember.

Sammendrag

Da er det kun innspurten igjen før det er en velfortjent pust i bakken for mange. Selv om det går mot jul legger ikke cyberkriminelle ned aktiviteten. Det har vært flere hendelser mot norske virksomheter den siste tiden, og kriminelle benytter gjerne «fridager» til å boltre seg i systemer der hvor de har fått tilgang.

Gjennom perioden fra august/september og frem til begynnelsen av desember har vi sett at løsepengevirus, som vi har vært mest bekymret for, virkelig har spredd om seg. Virksomheter som Inocean, Norsvin, Vestas, Helgelands blad, Choice Hotels og flere til har blitt utsatt for den type angrep. Konsekvensene blir for mange av virksomhetene store. Det blir gjerne nedetid i produksjon og store kostnader for å håndtere etterarbeidet for å få systemene i drift igjen i en bedre tilstand sikkerhetsmessig enn de var i forkant av angrepet.

Den siste tiden har det også vært en rekke forskjellige andre hendelser. En kritisk sårbarhet i Atlassians produkt Confluence, ble utnyttet i norske bedrifter og kryptominere og annen skadevare ble installert av hackere via denne sårbarheten. Det danske Hjemmeværnet ble i september gjort oppmerksom på at det var plassert filer på mailserveren deres av hackere som hadde utnyttet en kjent sårbarhet i Exchange, en problematikk vi har vært innom tidligere. I tidligere situasjonsbilder har det også blitt nevnt at vi fortsatt i lang tid vil se phishing, SMS-phishing knyttet til tema Korona/Vaksinering. Dette så vi eksempel på under denne perioden da flere Osloborgere mottok en SMS fra et telefonnummer som hevdet at de var fra Oslo kommune. Informasjonen omhandlet tredje vaksinedose.

EMOTET som tidligere har rammet flere norske kommuner, har K-CSIRT omtalt ved flere anledninger. EMOTET er en skadevare som spres ved hjelp av ondsinnede filer gjennom phishing. Den stjeler blant annet e-poster og bruker disse til å sende ut skadevare til nye mottakere som man har hatt e-postdialog med. Emotet har nå ligget brakk i nesten et år, dessverre ble nye e-postkampanjer observert 15. november med Excel eller Word- vedlegg som inneholder EMOTET-skadevare. K-CSIRT vil igjen understreke hvor viktig det er med god sikkerhet knyttet til e-post.

Man ser gjerne at når en kriminell aktør blir borte, dukker det opp igjen to nye. Aktørene blir flere og mer sofistikerte. Heldigvis ser det ut til at politiet i flere tilfeller er på sporet av kriminelle og klarer å ta dem. Spørsmålet vi stiller oss i «Situasjonsbilde og vurderinger» er: «Truslene fra de cyberkriminelle – er det noe lys i tunellen?»

Temabolken i dette «Situasjonsbilde» omhandler loggsentralisering med Logging Made Easy. Mange enheter i ett nettverk produserer logger som lagres lokalt. Disse loggene er viktige for å oppdage og analysere en hendelse. Lokal lagring utgjør en risiko ved at en angriper kan slette eller kryptere loggene før hendelsen oppdages. Sentralisering av loggene gjør hendelsesanalysen mer effektiv og reduserer risikoen for loggsletting, Artikkelen beskriver Logging Made Easy (LME) - en guide for installasjon og konfigurering av loggsentralisering utarbeidet av NCSC-UK (den britiske CERT-en).

Til slutt i «Situasjonsbildet» ser vi på hva som kan bidra til å skape utfordringer for oss i tiden som kommer. Nye phishingbølger, spredning av EMOTET og naturlig nok nye løsepengevirusangrep spesielt mot VA. Og migrering til sky kan være risikabelt hvis man ikke har god kompetanse og prioritet på sky-sikkerhet!

Hendelser

Hacking av et av USAs største telekommunikasjonsselskaper
16. august ble det kjent at T-Mobile, et av de største telekommunikasjonsselskapene i USA, var blitt hacket. I nærheten av 50 millioner nåværende, tidligere og potensielle kunder var kompromittert og det ble kjent at de kriminelle fikk tilgang til navn, adresser, personnummer, førerkort og ID-opplysninger for om lag 48 millioner mennesker. T-Mobile bruker begrepene "stjålet", "kompromittert", og "urettmessig tilgang til kontoer og data" om hverandre, så det er naturlig å anta at mange av disse opplysningene er på avveie. Senere har en 21 år gammel amerikaner tatt på ser ansvaret for ugjerningen og meddelt at det ble benyttet en usikret ruter for å oppnå tilgang.

Atlassian Confluence utnyttet i Norge
Nasjonal sikkerhetsmyndighet (NSM) meldte i begynnelsen av september om en kritisk sårbarhet i Atlassians produkt Confluence som ble utnyttet i norske bedrifter. Det var kryptominere og annen skadevare ble installert via denne sårbarheten. NSM meddelte videre at virksomheter som installerte sikkerhetsoppdateringer etter 31. august 2021, burde anta at eksponerte instanser av Confluence hadde vært utsatt for automatisert utnyttelse av sårbarheten, eksempelvis med forsøk på installasjon av kryptominer.

FBI med angrep mot REvil
I vår forrige rapport (no 2 – 2021) kunne man lese om at programvareleverandør Kaseya ble rammet av løsepengevirus. Senere (kjent i september) slo FBI tilbake mot REvil og fikk tak i en generell dekrypteringsnøkkel. Med bakgrunn i deres operasjon mot aktøren ventet de 3 uker med å gi nøkkelen til de rammede virksomhetene, blant annet Kaseya-kundene.

Dansk heimevern utsatte Exchange-oppdatering
Den 12. september i år ble informasjonssikkerhetssjefen i det danske Hjemmeværnet gjort oppmerksom på at det lå noen mistenkelige filer i styrkens Microsoft Exchange-system. De mistenkelige filene var blitt plassert der av hackere som hadde utnyttet en kjent sårbarhet i Exchange Server. Hackerne skal ha fått tilgang til systemene den 31. august. På dette tidspunktet hadde en sikkerhetsoppdatering som fjerner sårbarheten vært tilgjengelig i nesten to måneder.

REvils ransomware angrep mot Inocean
17. september publiserte Digi en artikkel om REvils ransomware angrep mot Inocean, hvilket foregikk 30. juli. REvils inngangsvektor var via en Phishing epost, hvor de så kompromitterte Inoceans-nettverket. Etter dette ventet de nærmere tre måneder før de tok i bruk kompromitterte kontoer og lagde spor av unormale påloggінger. Tre separate sikkerhetskopier ble delvis kryptert og data måtte hentes tilbake fra epost, PC-er som var offline under angrepet og vha Ibas. Inocean var tilbake i normal drift etter en måned. REvil listet angrepet på sine nettsider med påstand om å ha hentet ut 2TB med data.

Datatilsynet vil ikke ta i bruk Facebook
22. september kunngjorde Datatilsynet eget standpunkt til bruk av Facebook. Forvaltningsorganet vil ikke bruke Facebook i sitt kommunikasjonsarbeid. Avgjørelsen er basert på tilsynets egen risikovurdering. – Vi har valgt å ikke gå inn på Facebook fordi vi mener at behandlingen av personopplysninger medfører en for høy risiko for brukernes rettigheter og friheter, sa direktør Bjørn Erik Thon.

Sporveien utsatt for datainnbrudd
Tidlig i juli ble Sporveien hacket – ukjente eksterne hadde skaffet seg uautorisert tilgang til e-postkontoen til en medarbeider. Saken skjedde i juli, men ble først offentlig kjent 24. september ifølge Digi. Tilgangen har blant annet ført til forsøk på spam-utsendelse via denne kontoen. Selskapet uttale blant annet:

"Selskapet har «for lite informasjon og loggføring» til å kunne understøtte en etterforskning. Derfor er ikke saken politianmeldt".

Helgelands Blad utsatt for Ransomware
NRK meldte 28. september om at en norsk lokalavis ble hacket. Sitat fra ranablad.no: «Fikk ikke gitt ut avis for første gang siden krigen".

Innbyggere tilhørende Oslo kommune utsatt for SMS-phishing
Flere Osloborgere fikk mandag 11. oktober en SMS fra et telefonnummer som hevder at de var kommunen. Oslo kommune gikk ut med en advarsel om at det verserer en falsk SMS, som tilsynelatende kom med informasjon om en tredje vaksinedose. Mottakere av tekstmeldingen ble bedt om å svare med blant annet personnummer og fult navn.

Østre Toten kommune med bot fra Datatilsynet
19. oktober kunne vi lese om at et varsel fra Datatilsynet til Østre Toten kommune var sendt: Østre Toten kommune får fire millioner i bot etter dataangrepet. Dette er den største boten Datatilsynet noen gang har gitt en kommune. Tilsynet skriver i vedtaket at kommunen har hatt store mangler på grunnleggende sikkerhet, og de ser særlig alvorlig på at personopplysninger og opplysninger om barn er rammet av angrepet.

Universitet i Tromsø utsatt for dataangrep
19 oktober ble vi kjent med at det hadde vært et dataangrep mot Universitetet i Tromsø. Passordene til over 20 brukerkontoer ble stjålet i et dataangrep mot universitetet. Alle studenter og ansatte måtte bytte passord. Totalt rammet dette om lag 26.000 brukere. De kompromitterte kontoene ble raskt deaktivert, og universitetet uttalte at de ikke hadde noen indikasjoner på at data var blitt hentet ut.

Nettverket bak Hydro-angrepet arrestert
Ultimo oktober ble det kjent at de kriminelle bak Hydro-angrepet var arrestert. I en felles aksjon mellom seks europeiske land og Ukraina, ble det aksjonert mot 12 personer som skal ha stått bak 1800 angrep i 71 land, deriblant Hydroangrepet som kostet bedriften 800 millioner kroner.

Norsvin rammet av løsepengeangrep
5. november ble Norsvin utsatt for løsepengeangrep. Bedriftens datasystemer ble stengt ned. Selskapet fikk et varsel fra utpresserne om at de har gjort dataene deres utilgjengelige. Produksjonen gikk som normalt etter angrepet selv om e-post og systemet for ordrebestilling har vært ute av drift. Norsvin er et avlsselskap som driver avlsarbeid på svin i Norge.

Arrestasjon knyttes til REvils angrep på Kaseya i juli
8. november meldte det amerikanske justisdepartementet om at 22 år gamle Jaroslav Vasinski fra Ukraina er arrestert og siktet for å stå bak REvils angrep på Kaseya i juli (jf. Situasjonsbilde no2 – 2021). Samtidig har de siktet den 28 år gamle russiske statsborgeren Jevgeni Poljanin for å ha utført tilsvarende angrep på andre ofre i regi av REvil. Sistnevnte ble sporet opp ved å følge betalingsstrømmer for løsepengeangrep.

Nye EMOTET e-postkampanjer treffer verden over
EMOTET ser ut til å være tilbake. Nye e-postkampanjer ble observert 15. november med Excel eller Word-vedlegg som inneholder EMOTET-skadevare. EMOTET-programvare og nettverk ble angivelig 'utslettet' i april etter arrestasjoner og konfiskering av utstyr i januar i Ukraina. Etter en ti-måneders pause er altså EMOTET tilbake for å levere ondsinnede dokumenter til postbokser over hele verden.

Vestas utsatt for datainnbrudd med krav om løsepenger
Big game hunting er langt fra lagt ned: Vestas er verdens største produsent av vindturbiner med produksjonsanlegg i en lang rekke land, inkludert Norge. Det danske konsernet har nærmere 30.000 ansatte og en årsomsetning på mer enn 15 milliarder euro. 22. november skrev Vestas at hendelsen hadde påvirket deler av den interne IT-infrastruktur og at data var blitt kompromittert. Det var på dette tidspunktet imidlertid ingen indikasjoner på at hendelsen hadde påvirket tredjeparts operasjoner, inkludert kunde- og forsyningskjedeoperasjoner.

Nordic Choice Hotels rammet av løsepengeangrep
2. desember melder digi.no om at mer enn 200 hoteller til Nordic Choice Hotels i fem land er hardt rammet av et massivt cyberangrep/løsepengeangrep. Bleeping Computer og flere andre media melder noen dager senere at det er Conti som står bak, kanskje den mest aktive og avanserte aktøren blant de digitale utpresserne.

Situasjonsbilde og vurderinger:

Truslene fra de cyberkriminelle – er det noe lys i tunellen?
I slutten av oktober og begynnelsen av november fikk vi nyheter om at REvil/Sodinokibi var tatt (nok en gang) og at de kriminelle bak Hydro-angrepet var arrestert i en samordnet aksjon mellom mange land. REvil ble borte fra radaren i juli, rett etter Kaseya-angrepet som blant annet rammet COOP i Sverige, dukket så opp igjen og ble promotert av 'søster'-banden Conti som hevdet at de slettes ikke var ute av business. Så kom det nye angrep fra REvil, og deretter de siste arrestasjonene i begynnelsen av november som nevnt under 'Hendelser'. Nå har europeisk politi og FBI i tillegg til arrestasjonene også tatt ned infrastruktur og beslaglagt verdier i kryptovaluta. Så spørs det om de nok en gang gjenoppstår fra asken.

Av andre tilbakeslag for denne typen cyberkriminelle kan nevnes at det sveitsiske sikkerhetsfirmaet Prodaft klarte å hacke seg inn på nevnte Conti sine systemer og avsløre deler av deres infrastruktur. Det viser at selv de dyktigste og mest hardbarkede kriminelle også er sårbare.

Vår vurdering er at det store problemet med organisert cyberkriminalitet er at det dukker stadig opp nye aktører til tross for noen vellykkede politiaksjoner, noen ganger helt nye aktører og andre ganger avarter som mange mener kun er en rebranding av en eksisterende aktør. Tall fra de som overvåker dobbeltutpressingsaktørene på det mørke nettet (f.eks. DarkTracer) tyder på en dobling av antall trusselaktører i dette segmentet de siste 6 månedene, og bare i de to første ukene av november er det globalt registrert ca. 40 lekkasjer.

Vi vurderer det også som sannsynlig at de største kriminelle aktørene fremover vil være mer forsiktige og antagelig i større grad ligge unna de aller største virksomhetene og samfunnskritiske funksjonene for å unngå mer av den massive klappjakten som amerikanerne kjører mot REvil, DarkSide og andre som har rammet USA hardt. Dette *kan* utgjøre økt fare for at mindre virksomheter i andre vestlige land får en økning i antall angrep og kompromitteringer i tiden som kommer. Mange er også bekymret for sårbar OT (operasjonsteknologi) etter angrepet mot Colonial Pipeline i sommer. USA har opplevd en økning i angrepsvolum mot VA (Vann- og Avløp) i det siste, selv om det ikke nødvendigvis betyr økt målretting mot sektoren. Kombinasjonen økt fokus på mindre virksomheter og land - og sårbar operasjonsteknologi i kritisk infrastruktur - kan gjøre norske kommuner enda mer utsatt enn før.

I november kom det også observasjoner som tyder på at også EMOTET-skadevaren og botnettet er tilbake. Dette er en gruppering/skadevare som tilbyr phishing med nedlasting av skadevare via vedlegg, og hvor oppdraget videre kan variere fra kontosalg til ny phishing-spredning eller ransomware. Enkelte sikkerhetsfirma mener at tidligere nevnte trusselaktør Conti har en finger med i spillet rundt EMOTETs

gjenoppstandelse. Denne gjenoppstandelsen bekrefter teorien om et velutviklet samarbeid og løse knytninger og fragmenterte forsyningskjeder i disse kriminelle miljøene, som igjen gjør det enkelt for noen å ta opp tråden som andre har sluppet.

Samtidig ser vi fortsatt løsepengeangrep i Norge, de siste månedene har vi via vår trusseletterretning blitt kjent med et angrep mot en mellomstor bedrift i Rogaland, samt observert at Norsvin i Brumunddal ble tatt av løsepengeaktører i begynnelsen av november. Begge virksomheter fikk mye av infrastrukturen sin tatt ned og hadde nedetid på deler av tjenestene sine. Og desember måned starter med tilsvarende hendelse hos hotellkjeden Nordic Choice Hotels.

Vår vurdering er derfor at trusselen er like reell, til tross for flere vellykkede politiaksjoner mot disse miljøene i det siste. Fortsatt gjelder det å sikre systemene sine. Våre tre hovedanbefalinger er som før:

1. Komplett/tett multifaktorautentisering for alle brukere og systemer
2. Sørg for å ha offline backup som kan benyttes til restore/gjenoppretting av data
3. Sørg for et effektivt og årvåkent oppgraderings-/patcheregime

Bygg også opp gode løsninger for loggsentralisering og håndtering av uønsket trafikk og programvare.

Loggesentralisering med Logging Made Easy

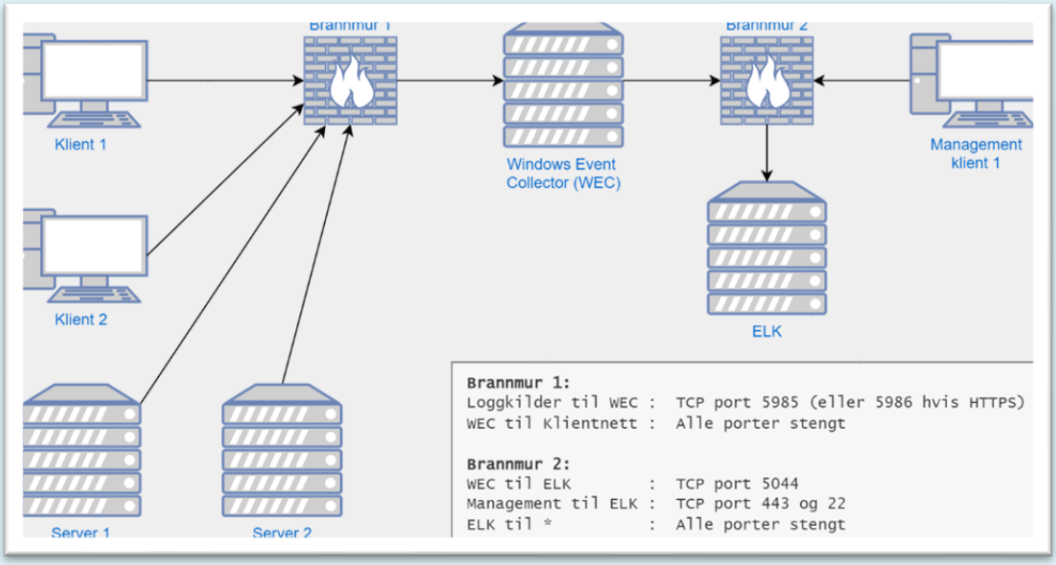
Mange enheter i ett nettverk produserer logger. Disse loggene kan gi sikkerhetsanalytikere kritisk innsikt for å oppdage og håndtere hendelser. Dessverre blir loggene ofte kun lagret på enhetene som produserer dem, noe som vanskeliggjør analyse og korrelasjon, og medfører en risiko dersom enhetene blir kryptert av løsepengevirus. Ved å automatisere innsamling av loggene omgås flere av disse problemene. Loggene sentraliseres på ett kontrollert sted hvor de er tilgjengelig over tid for både manuell og automatisk analyse. Vi anbefaler at logger lagres i minimum 6 måneder. Denne artikkelen gir en kort beskrivelse av ett system for loggsentralisering, samt noen anbefalinger og nyttig tips fra Kommune-CSIRT.

Logging Made Easy (LME) er en guide for installasjon og konfigurering av loggsentralisering. Den er skrevet av britiske NCSC, som er en del av GCHQ. Guiden beskriver hvordan en IT-organisasjon kan bruke funksjonalitet i programvare de alt har, sammen med programvare basert på åpen kildekode, til å produsere og sentralisere logger. I tillegg inneholder den prekonfigurerte dashbord som kan brukes for å se etter mistenkelig aktivitet, utdatert programvare, hvem som logger på hvor, m.m.

Før vi går videre er det verdt å nevne at LME ikke er en full erstatning for en SIEM-løsning, men ett viktig steg i riktig retting. Løsningen er beregnet på små til middels store organisasjoner som ikke har mulighet til å skaffe seg en SIEM-løsning. LME er gratis (gitt att man alt har Windows og litt ledig serverkapasitet), og man må derfor gjøre arbeidet selv for å ta den i bruk.

Forkunnskaper som anbefales er:

- installasjon av Windows Server og kobling til ett AD-domene
- deployering av GPOer eller annen metode for distribuering av konfigurasjon
- endring av brannmurregler
- installasjon og konfigurasjon av en Linux-maskin



Skissen over viser vår anbefaling for hvordan LME settes opp i nettverket, samt brannmurregler mellom de ulike maskinene. Dette vil selvfølgelig variere mellom organisasjoner. Noen nøkkelpunkter: klientnettverket må kunne snakke med WEC (Windows Event Collector), men kun en port er nødvendig, og WEC trenger ikke å kunne koble seg tilbake til klientene eller ut på internett for å motta logger. WEC og management klienter må kunne koble seg til ELK, men bare på noen få porter, og ELK trenger ikke å kunne nå noe som helst. Denne arkitekturen skalerer svært bra, med mulighet for å sette inn flere WEC-maskiner for å håndtere flere klienter eller klienter i ulike soner, og brannmurreglene reduserer angrepsflaten mellom de ulike enheten.

LME benytter Sysmon til å produsere logger på Windows klienter og Servere, og Windows Event Forwarding (WEF) til å sende dem til en Windows Event Collector. Konfigurasjon av hvilke Event Logger som skal sendes og oppsett av WEC distribueres via GPO. Disse templatene er inkludert i guiden. WEF kan konfigureres både som push, hvor kilden kobler seg til WEC og sender logger, og pull, hvor WEC kobler seg til kildene og henter loggene. Kommune-CSIRT anbefaler **push** konfigurasjon, da dette skalerer bedre i store nettverk. GPOene som ligger i LME gjør dette som standard, og linken om push-konfigurering under inneholder tips til feilsøking.

WEF overfører logger ved hjelp av WinRM protokollen, som bygger på HTTP. Både HTTP og HTTPS kan benyttes, og LME benytter HTTP som standard. Dette er ett av svært få tilfeller hvor vi i Kommune-CSIRT sier det er greit å bruke HTTP, da innholdet i meldingen som sendes blir kryptert vha. Kerberos. HTTPS har noen fordeler over HTTP i dette tilfellet, som f.eks. sertifikat-basert autentisering og tillate at maskiner som ikke er medlem av domenet kan sende inn logger, men krever litt mer konfigurering.

Til slutt i rekken står ELK-stacken. ELK står for Elasticsearch, Logstash og Kibana, som er åpen-kilde verktøy for å søke i, prosessere og visualisere logger. Denne maskinen kjøre ett Linux basert operativsystem, og bruker Docker til å forenkle installasjon og oppsett. Ubuntu LTS 20.04 anbefales som operativsystem, og er det vi har brukt i testing. LME inneholder ett script som installerer Docker, laster ned de riktige containerene, og starter opp tjenestene. Vi anbefaler derfor å starte med en helt ren Ubuntu installasjon, med mindre man har erfaring med Docker.

Kibana brukes for å søke i og visualisere logger. Webtjenesten kjører på ELK maskinen, og passordet for pålogging genereres under installasjon. Maskinen må derfor også være tilgjengelig fra management nettverk, eller tilsvarende, slik at loggene kan analyseres. LME kommer også med en rekke forhåndsdefinerte dashbord til f.eks. å se hvilke prosesser som kjører på hvilke maskiner og hvem som logger på hvor i nettverket. I tillegg har Kibana støtte for «Detection rules», som er regler som kjøres over innkommende logger og produserer alarmer. Reglene som ligger inne som standard oppdager f.eks. prosesser som startes på mistenkelige måter og forsøk på nettverksenumerering.

Helt til slutt vil vi ta med ett avsnitt om logg-retention, det vil si hvor lenge logger lagres og er søkbare. Å lagre logger over tid krever mye lagringsplass. Som standard, lager LME en retention-policy ved installasjon basert på å bruke 80% av ledig disk-kapasitet. Det vil si at den starter å overskrive logger når 80% av kapasiteten er brukt, uavhengig av hvor mange dager som har gått. Guiden beskriver hvordan dette kan endres, og man kan sette X antall dager eller Y antall GB. Her har vi ikke gjennomført grundige tester, da ulike maskiner og brukere produserer veldig forskjellig mengde logger. Vi ønsker tilbakemelding fra de som tar i bruk LME på hvor mye logger som produseres i gjennomsnitt per maskin, for å gjør det enklere for ande å planlegge lagringen sin.

Flere detaljer kommer frem i egen artikkel på kommunecsirt.no

Nyttige lenker:

Logging Made Easy (selve guiden): https://github.com/ukncsc/lme
Microsoft sin guide for oppsett av WEF: https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
ELK stacken: https://www.elastic.co/what-is/elk-stack

Glasskula – hva ser vi komme?

Denne utgaven av Digitalt Situasjonsbilde publiseres rett før jul. Man trenger ikke være sikkerhetsekspert for å hevde at nye phishingbølger vil komme i den nærmeste tiden f, særlig aktuelt er falske pakkesporinger både via SMS og e-post. Men gitt smittesituasjonen i pandemien, vil også vaksinasjon og smitteregler være aktuelle temaer for phishing. Lotterivarianter og etterligning av store nettbutikker og transportører vil også opptre i betydelige mengder.

Vi vil også advare mot EMOTET som tilsynelatende er tilbake. EMOTET er både et nettverk av infiserte systemer og en egen skadevare som lastes ned i forbindelse med datainnbrudd eller phishing. Både botnettet og skadevaren ble rapportert tatt ned og fjernet i våres. EMOTET ble ofte brukt til å stjele e-post-samtaler og så sende ut forfalskede meldinger som om de var en del av samtalen. Dette gjør forfalskningen vanskelig å avsløre, og vi vurderer som sannsynlig at flere kommuner kommer til å erfare EMOTET-angrep neste år.

Av det enda mer alvorlige slaget er at vannverk og VA-systemer kan bli rammet av avanserte løsepengeaktører som i verste fall forgifter eller stopper vannforsyning. Vannforsyning er definert som GNF (Grunnleggende Nasjonal Funksjon) av Helse- og omsorgsdepartementet og som kritisk infrastruktur av GDPR/EU. Vi advarer mot angrep på vannforsyning da vår vurdering er at disse etatenes systemer ofte er mindre beskyttet enn vanlig «kontor-IT». En større grad av spesialisering hos de kriminelle kan medføre mer målrettede angrep mot nettopp operasjonsteknologi (OT). Samtidig har denne typen systemer blitt utsatt for en økt angrepsfrekvens enn tidligere – blant annet i USA. Derfor jobber Kommune-CSIRT aktivt med medlemmene for å kartlegge sikkerheten i nettopp disse områdene i kommunen. Vår vurdering samlet sett er at disse systemene er mer utsatt enn før.

En mulig vridning av de avanserte kriminelles fokus fra de store globale selskapene til mindre virksomheter og land, kan ramme norske kommuner hardt. Vår vurdering er at mangel på betaling (ØT betalte ikke, det er bra!) og bedre sikkerhet vil bidra til å holde ondsinnede operasjoner unna, men noe vil nok treffe oss.

Til slutt vil vi uttrykke vår bekymring for mulige problemer ved norske kommuners migrering til sky – her i betydningen “Platform-as-a-Service" (PaaS)*. Bekymringen er først og fremst grunnet mulig manglende kompetanse og overdreven tro på at leverandørene beskytter mer enn de egentlig gjør. De fleste eksemplene på sårbarheter som oppstår etter en slik overgang, skyldes feilkonfigurering. Derfor må kunnskapen økes, hjelp anskaffes og overgangen kjøres som et godt planlagt prosjekt hvor sikkerhet er høyt prioritert. Vår vurdering er at det er sannsynlig at norske kommuner eller virksomheter innen offentlig forvaltning vil bli kompromittert som følge av sårbarheter ved overgang til sky i løpet av kommende år.

**)PaaS brukes når man ikke ønsker å kjøpe maskinvare for servere og anskaffe (bygge/leie/kjøpe) datasenter selv. Eksempler på leverandører er Microsoft (Azure) og Amazon (AWS). Hos disse kan man leie servere, operativsystem, nettverk og lagring. Man er selv ansvarlig for sikkerheten, og det finnes et stort tilbud av sikkerhetstjenester og mekanismer man kan kjøpe i tillegg til basistjenestene. Infrastructure-as-a-Service (IaaS) er nesten det samme og begrepene brukes ofte om hverandre, men for IaaS har kunden vanligvis også ansvar for å installere operativsystem og eventuell annen basis programvare (f.eks mellomvare).*

Siste side

Rapportens aktuelle situasjonstips:

Sikkerhetskultur og operasjonell sikkerhet:

- Ikke aktiver innhold i vedlegg og ikke klikk på lenker verken i epost eller SMS (uten å dobbeltsjekke med avsender)
- Ikke bruk jobbkonto til private formål
- Gjenbruk av brukernavn og passord er ingen god idé og må unngås!

De viktigste sikkerhetstiltakene:

- Sørg for multi-faktorautentisering for *all* tilgang utenfra
- Sørg for å ha sikkerhetskopier som er reelt offline, og testet for gjenoppretting
- Oppgrader alt internett-eksponert utstyr så raskt det lar seg gjøre - angrepene mot disse øker
- Ikke la utrangert utstyr bli stående eksponert mot internett

Relevante rapporter, dokumenter og kampanjer lansert i perioden:

NSM: Nasjonalt Digitalt Risikobilde 2021
https://nsm.no/getfile.php/137495-1635323653/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf

NorSIS: Nordmenn og digital sikkerhetskultur 2021
https://norsis.no/wp-content/uploads/1637/76/NorSIS_Nordmenn_og_digital_sikkerhetskultur_2021_Web.pdf

K-CSIRT ønsker å minne om viktige nasjonale prinsipper og strategier:

NSMs grunnprinsipper for IKT-sikkerhet:
https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

Nasjonal strategi for digital sikkerhet:
https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Tiltaksoversikt til Nasjonal Strategi for digital sikkerhet
https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/tiltaksoversikt---nasjonal-strategi-for-digital-sikkerhet.pdf

Kommune-CSIRT støtter sine medlemmer med råd, varsling og tiltak innenfor både strategisk og operativ informasjonssikkerhet. Vi støtter også medlemmene ved hendelser og fungerer som et bindeledd mellom tekniske hendelseshåndterere og virksomhetsledelse, og mellom ledelse og andre kommuner, sektorer og myndigheter. **Kontakt Kommune-CSIRT: post@kommunecsirt.no eller telefon 90 85 00 42.**